

BOUNDS ON EXPONENTIAL SUMS WITH QUADRINOMIALS

SIMON MACOURT

ABSTRACT. We improve an existing result on exponential quadrilinear sums in the case of sums over multiplicative subgroups of a finite field and use it to give a new bound on exponential sums with quadrinomials.

1. INTRODUCTION

1.1. Set Up. For a prime p , we use \mathbb{F}_p to denote the finite field of p elements.

For a t -sparse polynomial

$$\Psi(X) = \sum_{i=1}^t a_i X^{k_i}$$

with some pairwise distinct non-zero integer exponents k_1, \dots, k_t and coefficients $a_1, \dots, a_t \in \mathbb{F}_p^*$, and a multiplicative character χ of \mathbb{F}_p^* we define the sums

$$S_\chi(\Psi) = \sum_{x \in \mathbb{F}_p^*} \chi(x) \mathbf{e}_p(\Psi(x)),$$

where $\mathbf{e}_p(u) = \exp(2\pi i u/p)$ and χ is an arbitrary multiplicative character of \mathbb{F}_p^* . The challenge for such sums is to provide a bound that is stronger than the Weil bound

$$S_\chi(\Psi) \leq \max\{k_1, \dots, k_t\} p^{1/2},$$

see [18, Appendix 5, Example 12], by taking advantage of the arithmetic structure of the exponents. The case of exponential sums of monomials has seen much study with Shparlinski [16] providing the first such bound. Further improvements have been made by various other authors, see [1, 3, 11, 12, 15, 17]. We also mention that Cochrane, Coffelt and Pinner, as well as others, have given several bounds on exponential sums with sparse polynomials, see [4–9] and references therein, some of which we outline in Section 1.2.

2010 *Mathematics Subject Classification.* 11L07, 11T23.

Key words and phrases. exponential sum, sparse polynomial, quadrinomial.

Here we provide some new bounds on quadrinomial exponential sums using the techniques in [13]. We thus define

$$(1.1) \quad \Psi(X) = aX^k + bX^\ell + cX^m + dX^n.$$

We mention that all our results extend naturally to more general sums with polynomials of the shape

$$\Psi(X) = aX^k + f(X^\ell) + g(X^m) + h(X^n)$$

for polynomials $f, g, h \in \mathbb{F}_p[X]$.

The notation $A \ll B$ is equivalent to $|A| \leq c|B|$ for some constant c .

1.2. Previous Results. We compare our result for quadrinomials (1.1) to those of Cochrane, Coffelt and Pinner [4, Theorem 1.1]

$$S_\chi(\Psi) \ll \left(\frac{klmn}{\max(k, \ell, m, n)} \right)^{1/9} p^{8/9}$$

which is non-trivial for

$$\frac{klmn}{\max(k, \ell, m, n)} < p,$$

and of Cochrane and Pinner [6, Theorem 1.1]

$$S_\chi(\Psi) \ll (klmn)^{1/16} p^{7/8}$$

which is non-trivial for $klmn < p^2$. Our new result in Theorem 1.1 is independent of the size of the exponents but instead depends on various greatest common divisors.

1.3. Main Result. Our main result is the following theorem.

Theorem 1.1. *Let $\Psi(X)$ be a quadrinomial of the form (1.1) with $a, b, c, d \in \mathbb{F}_p^*$. Define*

$$\alpha = \gcd(k, p-1), \quad \beta = \gcd(\ell, p-1), \quad \gamma = \gcd(m, p-1), \quad \delta = \gcd(n, p-1)$$

and

$$f = \frac{\alpha}{\gcd(\alpha, \delta)}, \quad g = \frac{\beta}{\gcd(\beta, \delta)}, \quad h = \frac{\gamma}{\gcd(\gamma, \delta)}.$$

Suppose $f \geq g \geq h$, then $p/\delta \geq f$ and

$$S_\chi(\Psi) \ll pg^{-1/8} + \begin{cases} p^{15/16} \delta^{1/32}, & \text{if } g \geq p^{1/2} \log p, \\ p^{31/32} \delta^{1/32} g^{-1/16+o(1)}, & \text{if } f \geq p^{1/2} \log p > g, \\ p \delta^{1/32} (fg)^{-1/16+o(1)}, & \text{if } p/\delta \geq p^{1/2} \log p > f, \\ p^{31/32+o(1)} \delta^{3/32} (fg)^{-1/16}, & \text{if } p/\delta < p^{1/2} \log p. \end{cases}$$

We mention that our result is independent of the size of our powers k, l, m, n and is strongest when δ is small and f, g, h are large. As mentioned in the previous section, previous results become trivial for quadrinomials of large degree. It is easy to see that our bound is non-trivial and improves previous results for a wide range of exponents k, ℓ, m and n .

2. PRELIMINARIES

We recall the following classical bound of bilinear sums, see, for example, [2, Equation 1.4] or [10, Lemma 4.1].

Lemma 2.1. *For any sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_p$ and any $\alpha = (\alpha_x)_{x \in \mathcal{X}}$, $\beta = (\beta_y)_{y \in \mathcal{Y}}$, with*

$$\sum_{x \in \mathcal{X}} |\alpha_x|^2 = A \quad \text{and} \quad \sum_{y \in \mathcal{Y}} |\beta_y|^2 = B,$$

we have

$$\left| \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \alpha_x \beta_y \mathbf{e}_p(xy) \right| \leq \sqrt{pAB}.$$

We define $D_{\times}(\mathcal{U})$ to be the number of solutions of

$$(u_1 - v_1)(u_2 - v_2) = (u_3 - v_3)(u_4 - v_4), \quad u_i, v_i \in \mathcal{U}, \quad i = 1, 2, 3, 4.$$

We also define the multiplicative energy $E^{\times}(\mathcal{U}, \mathcal{V})$ to be the number of solutions of

$$u_1 v_1 = u_2 v_2 \quad u_i \in \mathcal{U}, \quad v_i \in \mathcal{V}, \quad i = 1, 2.$$

When $\mathcal{U} = \mathcal{V}$, we write $E^{\times}(\mathcal{U}, \mathcal{U}) = E^{\times}(\mathcal{U})$.

We need the following result from [13, Corollary 3.3].

Lemma 2.2. *For a multiplicative subgroup $\mathcal{G} \subset \mathbb{F}_p^*$, we have*

$$D_{\times}(\mathcal{G}) \ll \begin{cases} |\mathcal{G}|^8 p^{-1}, & \text{if } |\mathcal{G}| \geq p^{1/2} \log p, \\ |\mathcal{G}|^6 \log |\mathcal{G}|, & \text{if } |\mathcal{G}| < p^{1/2} \log p. \end{cases}$$

We also use [13, Corollary 4.1].

Lemma 2.3. *Let \mathcal{G} be a multiplicative subgroup of \mathbb{F}_p^* . Then for any $\lambda \in \mathbb{F}_p^*$, we have*

$$E^{\times}(\mathcal{G} + \lambda) - \frac{|\mathcal{G}|^4}{p} \ll \begin{cases} p^{1/2} |\mathcal{G}|^{3/2}, & \text{if } |\mathcal{G}| \geq p^{2/3}, \\ |\mathcal{G}|^3 p^{-1/2}, & \text{if } p^{2/3} > |\mathcal{G}| \geq p^{1/2} \log p, \\ |\mathcal{G}|^2 \log |\mathcal{G}|, & \text{if } |\mathcal{G}| < p^{1/2} \log p. \end{cases}$$

We immediately obtain the following result by observing the dominant term from Lemma 2.3.

Corollary 2.4. *Let \mathcal{G} be a multiplicative subgroup of \mathbb{F}_p^* . Then for any $\lambda \in \mathbb{F}_p^*$, we have*

$$E^\times(\mathcal{G} + \lambda) \ll \begin{cases} |\mathcal{G}|/p, & \text{if } |\mathcal{G}| \geq p^{1/2} \log p, \\ |\mathcal{G}|^2 \log |\mathcal{G}|, & \text{if } |\mathcal{G}| < p^{1/2} \log p. \end{cases}$$

We define $N(\mathcal{F}, \mathcal{G}, \mathcal{H})$ to be the number of triples of solutions to $f_1(g_1 - g_2) = f_2(h_1 - h_2)$ where $f_i \in \mathcal{F}, g_i \in \mathcal{G}, h_i \in \mathcal{H}$ for $i = 1, 2$. Using Corollary 2.4 we obtain the following result.

Lemma 2.5. *Let $\mathcal{F}, \mathcal{G}, \mathcal{H}$ be multiplicative subgroups of \mathbb{F}_p^* with cardinalities F, G, H respectively with $G \geq H$. Additionally, let $M = \max(F, G)$. Then*

$$N(\mathcal{F}, \mathcal{G}, \mathcal{H}) \ll \frac{F^2}{M^{1/2}} \begin{cases} G^2 H^2 p^{-1/2}, & \text{if } H \geq p^{1/2} \log p, \\ G^2 H^{3/2+o(1)} p^{-1/4}, & \text{if } G \geq p^{1/2} \log p > H, \\ (GH)^{3/2+o(1)}, & \text{if } G < p^{1/2} \log p. \end{cases}$$

Proof. By multiplying both sides of $f_1(g_1 - g_2) = f_2(h_1 - h_2)$ by the inverses f_2^{-1} and h_2^{-1} and taking a factor of g_2 from the left hand side, and defining $S = \{fgh : f \in \mathcal{F}, g \in \mathcal{G}, h \in \mathcal{H}\}$ we have

$$N(\mathcal{F}, \mathcal{G}, \mathcal{H}) = \frac{F^2 GH}{|S|} \sum_{\lambda \in S} |\{\lambda(g-1) = h-1 : g \in \mathcal{G}, h \in \mathcal{H}\}|.$$

By the Cauchy inequality,

$$\begin{aligned} N(\mathcal{F}, \mathcal{G}, \mathcal{H})^2 &\leq \frac{F^4 G^2 H^2}{|S|} \left| \left\{ \frac{h_1 - 1}{g_1 - 1} = \frac{h_2 - 1}{g_2 - 1} : h_i \in \mathcal{H}, g_i \in \mathcal{G}, i = 1, 2 \right\} \right| \\ &= \frac{F^4 G^2 H^2}{|S|} (E^\times(\mathcal{G} - 1) E^\times(\mathcal{H} - 1))^{1/2}. \end{aligned}$$

By Corollary 2.4,

$$N(\mathcal{F}, \mathcal{G}, \mathcal{H})^2 \ll \frac{F^4 G^2 H^2}{|S|} \begin{cases} G^2 H^2 / p, & \text{if } H \geq p^{1/2} \log p, \\ G^2 H^{1+o(1)} p^{-1/2}, & \text{if } G \geq p^{1/2} \log p > H, \\ (GH)^{1+o(1)}, & \text{if } G < p^{1/2} \log p. \end{cases}$$

Since $|S| \geq M$ we complete our proof. \square

Applying Lemma 2.2 and Lemma 2.5 in the proof of [14, Theorem 1.4], we obtain the following result on quadrilinear sums over subgroups.

Lemma 2.6. *For any multiplicative subgroups $\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z} \subseteq \mathbb{F}_p^*$ of cardinalities W, X, Y, Z , respectively, with $W \geq X \geq Y \geq Z$ and weights $\vartheta = (\vartheta_{w,x,y})$, $\rho = (\rho_{w,x,z})$, $\sigma = (\sigma_{w,y,z})$ and $\tau = (\tau_{x,y,z})$ with*

$$\max_{(w,x,y) \in \mathcal{W} \times \mathcal{X} \times \mathcal{Y}} |\vartheta_{w,x,y}| \leq 1, \quad \max_{(w,x,y) \in \mathcal{W} \times \mathcal{X} \times \mathcal{Z}} |\rho_{w,x,z}| \leq 1,$$

$$\max_{(w,x,y) \in \mathcal{W} \times \mathcal{Y} \times \mathcal{Z}} |\sigma_{w,y,z}| \leq 1, \quad \max_{(w,x,y) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}} |\tau_{x,y,z}| \leq 1,$$

for the sums

$$T = \sum_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \sum_{z \in \mathcal{Z}} \vartheta_{w,x,y} \rho_{w,x,z} \sigma_{w,y,z} \tau_{x,y,z} \mathbf{e}_p(awxyz)$$

we have

$$|T| \ll WXYZ^{7/8} + \begin{cases} W^{31/32}XYZp^{-1/32}, & \text{if } Y \geq p^{1/2} \log p, \\ W^{31/32}XY^{15/16+o(1)}Z, & \text{if } X \geq p^{1/2} \log p > Y, \\ W^{31/32}(XY)^{15/16+o(1)}Zp^{1/32}, & \text{if } W \geq p^{1/2} \log p > X, \\ W^{29/32+o(1)}(XY)^{15/16}Zp^{1/16}, & \text{if } W < p^{1/2} \log p. \end{cases}$$

uniformly over $a \in \mathbb{F}_p^*$.

Proof. We see from [14, p. 24] that

$$|T|^8 \ll (WXY)^6 Z^7 \sum_{\mu \in \mathbb{F}_p^*} \sum_{\lambda \in \mathbb{F}_p} J(\mu) I(\lambda) \eta_\mu \mathbf{e}_p(\lambda \mu) + (W X Z)^8 Y^7,$$

where η_μ , $\mu \in \mathbb{F}_p^*$ is a complex number with $|\eta_\mu| = 1$, $J(\mu)$ is the number of quadruples $(x_1, x_2, y_1, y_2) \in \mathcal{X}^2 \times \mathcal{Y}^2$ such that $(x_1 - x_2)(y_1 - y_2) = \mu \in \mathbb{F}_p^*$ and $I(\lambda)$ is the number of triples $(w_1, w_2, z) \in \mathcal{W}^2 \times \mathcal{Z}$ such that $z(w_1 - w_2) = \lambda \in \mathbb{F}_p$. We estimate $J(\mu)$ as in [14, Equation 3.10] but using our bound from Lemma 2.2 to obtain

$$(2.1) \quad \sum_{\mu \in \mathbb{F}_p^*} J(\mu)^2 \ll \begin{cases} X^4 Y^4 / p, & \text{if } Y \geq p^{1/2} \log p, \\ X^4 Y^{3+o(1)} p^{-1/2}, & \text{if } X \geq p^{1/2} \log p > Y, \\ (XY)^{3+o(1)}, & \text{if } X < p^{1/2} \log p. \end{cases}$$

Now

$$\begin{aligned} & \sum_{\lambda \in \mathbb{F}_p} I(\lambda)^2 \\ &= |\{z_1(w_1 - w_2) = z_2(w_3 - w_4) : w_1, w_2 \in \mathcal{W}, z_i \in \mathcal{Z}, i = 1, 2, 3, 4\}| \\ &= N(Z, W, W). \end{aligned}$$

Therefore, by Lemma 2.5,

$$(2.2) \quad \sum_{\lambda \in \mathbb{F}_p} I(\lambda)^2 \ll \begin{cases} Z^2 W^{7/2} p^{-1/2}, & \text{if } W \geq p^{1/2} \log p, \\ Z^2 W^{5/2+o(1)}, & \text{if } W < p^{1/2} \log p. \end{cases}$$

Applying the classical bound on bilinear exponential sums from Lemma 2.1 together with (2.1) and (2.2), we get

$$|T|^8 \ll (WXZ)^8 Y^7 + \begin{cases} W^{31/4} X^8 Y^8 Z^8 p^{-1/4}, & \text{if } Y \geq p^{1/2} \log p, \\ W^{31/4} X^8 Y^{15/2+o(1)} Z^8, & \text{if } X \geq p^{1/2} \log p > Y, \\ W^{31/4} X (YZ)^{15/2+o(1)} Z^8 p^{1/4}, & \text{if } W \geq p^{1/2} \log p > X, \\ W^{29/4+o(1)} (XY)^{15/2} Z^8 p^{1/2}, & \text{if } W < p^{1/2} \log p. \end{cases}$$

Hence,

$$|T| \ll WXYZ^{7/8} + \begin{cases} W^{31/32} XYZ p^{-1/32}, & \text{if } Y \geq p^{1/2} \log p, \\ W^{31/32} XY^{15/16+o(1)} Z, & \text{if } X \geq p^{1/2} \log p > Y, \\ W^{31/32} (XY)^{15/16+o(1)} Z p^{1/32}, & \text{if } W \geq p^{1/2} \log p > X, \\ W^{29/32+o(1)} (XY)^{15/16} Z p^{1/16}, & \text{if } W < p^{1/2} \log p. \end{cases}$$

This completes the proof. \square

We compare our bound for subgroups from Lemma 2.6 with that for arbitrary sets coming from [14, Theorem 1.4]

$$(2.3) \quad \left| \sum_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \sum_{z \in \mathcal{Z}} \vartheta_{w,x,y} \rho_{w,x,z} \sigma_{w,y,z} \tau_{x,y,z} \mathbf{e}_p(awxyz) \right| \ll p^{1/16} W^{15/16} (XY)^{61/64} Z^{31/32}.$$

For example, if $W = X = Y = Z = p^{1/2+o(1)}$ then the bounds become $p^{125/64+o(1)}$ and $p^{63/32+o(1)}$ respectively.

3. PROOF OF THEOREM 1.1

Let $\mathcal{G}_\alpha, \mathcal{G}_\beta, \mathcal{G}_\gamma$ be the subgroups of \mathbb{F}_p^* formed by the elements of orders α, β and γ respectively. Then,

$$\begin{aligned} S_\chi(\Psi) &= \frac{1}{\alpha\beta\gamma} \sum_{x \in \mathcal{G}_\alpha} \sum_{y \in \mathcal{G}_\beta} \sum_{z \in \mathcal{G}_\gamma} \sum_{w \in \mathbb{F}_p^*} \chi(wxyz) \mathbf{e}_p(\Psi(wxyz)) \\ &= \frac{1}{\alpha\beta\gamma} \sum_{x \in \mathcal{G}_\alpha} \sum_{y \in \mathcal{G}_\beta} \sum_{z \in \mathcal{G}_\gamma} \sum_{w \in \mathbb{F}_p^*} \chi(wxyz) \mathbf{e}_p(aw^k y^k z^k + bw^\ell x^\ell z^\ell + cw^m x^m y^m + dw^n x^n y^n z^n) \\ &= \frac{1}{\alpha\beta\gamma} \sum_{x \in \mathcal{G}_\alpha} \sum_{y \in \mathcal{G}_\beta} \sum_{z \in \mathcal{G}_\gamma} \sum_{w \in \mathbb{F}_p^*} \vartheta_{w,x,y} \rho_{w,x,z} \sigma_{w,y,z} \mathbf{e}_p(dw^n x^n y^n z^n) \end{aligned}$$

where $\vartheta_{w,x,y} = \chi(wxy) \mathbf{e}_p(cw^m x^m y^m)$, $\rho_{w,x,z} = \chi(z) \mathbf{e}_p(bw^\ell x^\ell z^\ell)$ and $\sigma_{w,y,z} = \mathbf{e}_p(aw^k y^k z^k)$. Now the image $\mathcal{W} = \{w^n : w \in \mathbb{F}_p^*\}$ of non-zero n th powers contains $(p-1)/\delta$ elements, each appearing with multiplicity δ . Similarly, we can see that the images $\mathcal{X} = \{x^n : x \in \mathcal{G}_\alpha\}$, $\mathcal{Y} = \{y^n : y \in \mathcal{G}_\beta\}$ and $\mathcal{Z} = \{z^n : z \in \mathcal{G}_\gamma\}$ contain f, g and h elements with multiplicity $\gcd(\alpha, \delta)$, $\gcd(\beta, \delta)$ and $\gcd(\gamma, \delta)$ respectively. We apply Lemma 2.6, recalling our assumption that $f \geq g$ and noticing $f\delta = \text{lcm}(\alpha, \delta) < p-1$, hence $f \leq p/\delta$, which gives us

$$\begin{aligned}
S_\chi(\Psi) &\ll \frac{\delta \gcd(\alpha, \delta) \gcd(\beta, \delta) \gcd(\gamma, \delta)}{\alpha \beta \gamma} (p/\delta) f g^{7/8} h \\
&\quad + \frac{\delta \gcd(\alpha, \delta) \gcd(\beta, \delta) \gcd(\gamma, \delta)}{\alpha \beta \gamma} \\
&\quad \times \begin{cases} (p/\delta)^{31/32} f g h p^{-1/32}, & \text{if } g \geq p^{1/2} \log p, \\ (p/\delta)^{31/32} f g^{15/16+o(1)} h, & \text{if } f \geq p^{1/2} \log p > g, \\ (p/\delta)^{31/32} (f g)^{15/16+o(1)} h p^{1/32}, & \text{if } p/\delta \geq p^{1/2} \log p > f, \\ (p/\delta)^{29/32+o(1)} (f g)^{15/16} h p^{1/16}, & \text{if } p/\delta < p^{1/2} \log p. \end{cases} \\
&= p g^{-1/8} \\
&\quad + \begin{cases} p^{15/16} \delta^{1/32}, & \text{if } g \geq p^{1/2} \log p, \\ p^{31/32} \delta^{1/32} g^{-1/16+o(1)}, & \text{if } f \geq p^{1/2} \log p > g, \\ p \delta^{1/32} (f g)^{-1/16+o(1)}, & \text{if } p/\delta \geq p^{1/2} \log p > f, \\ p^{31/32+o(1)} \delta^{3/32} (f g)^{-1/16}, & \text{if } p/\delta < p^{1/2} \log p. \end{cases}
\end{aligned}$$

This concludes the proof.

REFERENCES

- [1] J. Bourgain, ‘Multilinear exponential sums in prime fields under optimal entropy condition on the sources’, *Geom. and Funct. Anal.*, **18** (2009), 1477–1502.
- [2] J. Bourgain and M. Z. Garaev, ‘On a variant of sum-product estimates and explicit exponential sum bounds in prime fields’, *Math. Proc. Cambridge Phil. Soc.*, **146** (2009), 1–21.
- [3] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, ‘Estimates for the number of sums and products and for exponential sums in fields of prime order’, *J. Lond. Math. Soc.*, **73** (2006), 380–398.
- [4] T. T. Cochrane, J. Coffelt and C. G. Pinner, ‘A further refinement of Mordell’s bound on exponential sums’, *Acta Arith.*, **116** (2005), 35–41.
- [5] T. T. Cochrane, J. Coffelt and C. G. Pinner, ‘A system of simultaneous congruences arising from trinomial exponential sums’, *J. Theorie des Nombres, Bordeaux.*, **18** (2006), 59–72.
- [6] T. Cochrane and C. Pinner, ‘An improved Mordell type bound for exponential sums’, *Proc. Amer. Math. Soc.*, **133** (2005), 313–320.

- [7] T. Cochrane and C. Pinner, ‘Using Stepanov’s method for exponential sums involving rational functions’, *J. Number Theory*, **116** (2006), 270–292.
- [8] T. Cochrane and C. Pinner, ‘Bounds on fewnomial exponential sums over \mathbb{Z}_p ’, *Math. Proc. Camb. Phil. Soc.*, **149** (2010), 217–227.
- [9] T. Cochrane and C. Pinner, ‘Explicit bounds on monomial and binomial exponential sums’, *Quart. J. Math.*, **62** (2011), 323–349.
- [10] M. Z. Garaev, ‘Sums and products of sets and estimates of rational trigonometric sums in fields of prime order’, *Russian Math. Surveys*, **65** (2010), 599–658 (Transl. from *Uspekhi Mat. Nauk*).
- [11] D. R. Heath-Brown and S. V. Konyagin, ‘New bounds for Gauss sums derived from k th powers, and for Heilbronn’s exponential sum’, *Quart. J. Math.*, **51** (2000), 221–235.
- [12] S. V. Konyagin, ‘Bounds of exponential sums over subgroups and Gauss sums’, *Proc. 4th Intern. Conf. Modern Problems of Number Theory and Its Applications*, Moscow Lomonosov State Univ., Moscow, 2002, 86–114 (in Russian).
- [13] S. Macourt, I. D. Shkredov, I. E. Shparlinski, ‘Multiplicative energy of shifted subgroups and bounds on exponential sums with trinomials in finite fields’, 2017 (available from <https://arxiv.org/abs/1701.06192>).
- [14] G. Petridis and I. E. Shparlinski, ‘Bounds on trilinear and quadrilinear exponential sums’, *J. d’Analyse Math.*, (to appear).
- [15] I. D. Shkredov, ‘On exponential sums over multiplicative subgroups of medium size’, *Finite Fields and Appl.*, **30** (2014), 72–87.
- [16] I. E. Shparlinski, ‘On bounds of Gaussian sums’, *Matem. Zametki*, **50** (1991), 122–130 (in Russian).
- [17] Y. N. Shteinikov, ‘Estimates of trigonometric sums over subgroups and some of their applications’, *Matem. Zametki*, **98** (2015), 606–625 (in Russian).
- [18] A. Weil, *Basic number theory*, Springer-Verlag, New York, 1974.

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES,
SYDNEY, NSW 2052, AUSTRALIA

E-mail address: `s.maccourt@student.unsw.edu.au`